REMARKS

Claims 3, 9, 29 and 35 have been amended to clarify the subject matter regarded as the invention. Claims 3, 4, 9, 29, 30 and 35 are pending.

The Examiner has rejected claims 3, 4, 9, 29, 30 and 35 under 35 U.S.C. §102(e) as anticipated by Crosbie et al.

The rejection is respectfully traversed. With respect to claim 3, Crosbie et al teach searching for attack patterns to detect exploits. However, Crosbie et al do not describe using a regular expression query to search for a pattern associated with a sgid exploit "in which a sgid process is used to spawn another process and...searching for entries showing that a process has been started by a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero," as recited in claim 3. Support for the amendment to claim 3 may be found, without limitation, in the Application at page 60, lines 4-19 and Figure 26. As such, claim 3 is believed to be allowable.

Claim 4 depends from claim 3 and is believed to be allowable for the same reasons described above.

Similarly to claim 3, claim 9 describes using a regular expression query to search for a pattern associated with a sgid exploit "in which a sgid process is used to spawn another process...wherein the shell comprises a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero," as recited in claim 9. As such, claim 9 is believed to be allowable for the same reasons described above.

Claim 29 recites a system for carrying out the method of claim 3. Therefore, it is believed that claim 29 is also allowable.

Claim 30 depends from claim 29 and is believed to be allowable for the same reasons described above.

Claim 35 recites program code for carrying out the method of claim 3. Therefore, it is believed that claim 35 is also allowable.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: 5/23/05

William J. James
Registration No. 40,661
V 408-973-2592
F 408-973-2595

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014